REMARKS

The above-identified patent application has been reviewed in light of the Examiner's Action dated December 3, 2004. Claims 1, 5, 7, 13 and 19 have been amended without intending to abandon or to dedicate to the public any patentable subject matter. No claims have been canceled. Therefore, Claims 1-21 are now pending. As set out more fully below, reconsideration and withdrawal of the objections to and rejections of the claims are respectfully requested.

The Office Action requires new corrected drawings because the drawings originally filed are informal. Formal drawings are provided with the Submission of Formal Drawings submitted herewith. Accordingly, reconsideration and withdrawal of the requirement for corrected drawings is respectfully requested.

The specification stands objected to as failing to provide proper antecedent basis for the claimed subject matter. In particular, the Office Action finds that the specification does not teach the limitation of Claim 7. In the amendments set forth above, the specification has been amended to incorporate the limitation of Claim 7. No new matter has been added to the application by this amendment. Accordingly, reconsideration and withdrawal of the objection to the specification is respectfully requested.

Claim 7 stands objected to on the grounds that the specification does not teach all of the limitations of that claim. As noted above, the specification has been amended to incorporate the limitations of Claim 7. In addition, Applicants note that the Office Action did not reject Claim 7 in view of any prior art. In the amendments set forth above, Claim 7 has been rewritten in independent form by incorporating the elements recited by original Claim 1. Applicants further note that in rewriting Claim 7 in independent form, the recitation of "said communications system" in original Claim 1, which was found to be indefinite, has been changed to "said communications server." Accordingly, reconsideration and withdrawal of the objection to Claim 7 are respectfully requested.

Claims 1-12 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that Applicants regard as the invention. In the amendments set forth above, the portion of Claim 1 noted as being

indefinite has been deleted. Accordingly, reconsideration and withdrawal of the rejection of Claim 1 and the claims dependent therefrom as indefinite should be reconsidered and withdrawn.

Claims 1, 3, 9-11, 13 and 14 stand rejected under 35 U.S.C. §102 as being anticipated by U.S. Patent No. 5,706,349 to Aditham et al. ("Aditham"). In order for a rejection under 35 U.S.C. §102 to be proper, each and every element as set forth in a claim must be found, either expressly or inherently described, in a single prior art reference. (MPEP §2131.) However, each and every element of the claims cannot be found in the Aditham reference. Therefore, reconsideration and withdrawal of the rejections of Claims 1, 3, 9-11, 13 and 14 are respectfully requested.

The present invention is generally directed to providing communications security using a remote server. Accordingly, various embodiments of the claimed invention provide for the generation of a token in a server, such as a communications server, and the provision of that token to a communications device. The communications device may add information and submit the token and additional information to a security server. The security server may then encrypt the token, and return the encrypted token to the communication device. The communication device then provides the encrypted token to the communications server. The communications server may then decrypt the token and determine whether the decrypted token received from the communications device matches the token that was provided to the communications device by the communications server.

The Aditham reference is generally directed to authenticating remote users in a distributed environment. More particularly, Aditham discusses a security protocol according to which a security process (the "SOMDD process") generates a random string or token in response to the receipt of a valid login name and password from a client. (Aditham, col. 6, ll. 4-14.) The security protocol process then passes the token back to the remote client, thereby authenticating the remote client or user. Following receipt of the token, the remote client may connect to an application server and provide the token to that application server. (Aditham, col. 6, ll. 24-30.) The application server then makes a call to the security process to verify whether the security process really issued the token for use with the user name and password provided by the remote client. (Aditham, col. 6, ll. 30-34.) If the security process finds that the string comprising the

token matches the token that was issued by the security process, the security process so notifies the application server. (Aditham, col. 6, ll. 35-41.) Accordingly, it can be appreciated that the token in the system discussed by Aditham originates in a security process, not with the application. Accordingly, Aditham does not describe a system in which a token is generated in a communications server. In addition, the Aditham reference does not describe a system in which an encrypted token is decrypted by a communications server or in which a communications server determines whether the decrypted token matches the token that it originally generated. Instead, Aditham discusses a system in which a security process must determine whether a token is authentic.

Claim 1 recites a method for providing communications system security. Elements recited by Claim 1 include "generating a token in said communications server; [and] providing said token to said first communications device." Claim 1 additionally recites "providing said identifying information and said token to said security server; [and] encrypting said token in said security server." Claim 1 further recites "providing said encrypted token to said first communications device; [and] providing said encrypted token from said first communications device to said communications server." According to Claim 1, the method also includes "decrypting said encrypted token received at said communications server; and determining at said communications server whether said decrypted token received at said communications server matches said token generated by said communications server." As noted above, Aditham does not describe a system in which a token is generated by a communications server. In addition, Aditham does not describe a system in which a token generated by a communications server is encrypted by a security server, and in which the encrypted token is passed to the communications server by the communications device. Furthermore, Aditham does not describe a system in which an encrypted token is received by a communications server and decrypted by that communications server. Also, the Aditham reference does not describe a system in which the communications server determines whether the decrypted token matches the token generated by the communications server. Accordingly, for at least these reasons, Claim 1 and the claims dependent therefrom are not anticipated by Aditham, and the rejections of these claims should be reconsidered and withdrawn.

Claim 13 is generally directed to a communications system providing remote security. The communications system generally includes a communications network, a system server, a communications device, and a security server. Furthermore, amended Claim 13 recites:

> wherein said system server provides said first communications device with a first token, wherein said first communications device provides said first token to said security server, wherein said security server encrypts said first token, wherein said first communications device provides said encrypted first token to said system server, and wherein said first communications device is granted access to said system server in response to receipt by said system server of said encrypted first token.

As noted above, the Aditham reference does not describe a system in which a system server generates a token that is provided to a security server by a first communication device. In addition, Aditham does not describe a system in which a token received by a security system is encrypted by that security system and returned to the communication device as an encrypted token. Furthermore, Aditham does not describe a system in which a communication device provides an encrypted token to a system server, and in which the system server decrypts the encrypted token and compares the decrypted token to the token that was originally provided by the system server to the communication device. Accordingly, for at least these reasons, Claim 13 and dependent Claim 14 are not anticipated by Aditham.

Claims 2, 4-6, 8, 12 and 15-21 stand rejected as obvious over 35 U.S.C. §103 over Aditham in view of U.S. Patent No. 5,978,918 to Scholnick et al. ("Scholnick"), Aditham in view of U.S. Patent No. 6,681,252 to Schuster et al. ("Schuster") and/or U.S. Patent No. 6,058,187 to Chen ("Chen"). In order to establish a prima facie case of obvious under section 103, there must be some suggestion or motivation to modify the reference or to combine the reference teachings, there must be a reasonable expectation of success, and the prior art reference or references must teach or suggest all of the claim limitations. (MPEP §2143.) Because each and every element of the invention as claimed cannot be found in the cited references, as set forth more fully below, the rejections under 35 U.S.C. §103 should be reconsidered and withdrawn.

Claims 2, 4-6, 8 and 12 generally depend from Claim 1. As noted above, a number of elements recited by Claim 1 are not described by the Aditham reference. Furthermore, the

recited elements missing from Aditham cannot be found in the cited references. For example, the Scholnick reference, which is cited by the Office Action for teaching a security system that utilizes identifying information as an encryption key, does not teach, suggest or disclose a token generated in a communications server that is passed to a security server by a communication device for decryption. Furthermore, Scholnick does not teach, suggest or describe providing an encrypted token from a security server to a communication device, which in turn provides the encrypted token to the communications server for decryption and validation. Instead, Scholnick discusses a system that requires the transmission of data outside of the public Internet in which a process generating a token also encrypts that token before providing it to another network node. Accordingly, for at least these reasons, Claim 2 is not obvious over the proposed combination of the Aditham and Scholnick references.

The Schuster reference is generally directed to a system and method for interconnecting portable information devices through a network based telecommunications system. The Office Action cites to Schuster in connection with various claim elements related to the transfer of communications extensions and features. However, Schuster does not teach, suggest or describe a method for providing communications system security in which the generation, encryption, decryption and validation of tokens are distributed as claimed. Therefore, for at least these reasons, the rejections of Claims 4-8 should be reconsidered and withdrawn.

The Chen reference is generally directed to secure telecommunications data transmission. In particular, Chen discusses an encryption device that operates to encrypt a message prior to forwarding the message to a remote destination. (Chen, col. 2, ll. 40-49.) However, a method or system in which the generation, encryption, decryption and validation of tokens are distributed as claimed is not taught, suggested or disclosed by Chen.

Claim 19 is generally directed to a communications system with security features. As amended, Claim 19 recites "means for providing communications services . . . wherein said means for providing communications services includes means for generating a first token." In addition, amended Claim 19 recite "means for encrypting said first token . . ., wherein said first token is received by said means for encrypting from said at least a first communications device, wherein said means for encrypting are located remotely from said at least a first communications

device." As noted above, neither the Aditham nor the Chen references teach, suggest or describe a system with token and encryption functions distributed as set forth in Claim 19. Accordingly, the rejection of Claim 19 and the claims dependent therefrom should be reconsidered and withdrawn.

The application now appearing to be in form for allowance, early notification of same is respectfully requested. The Examiner is invited to contact the undersigned by telephone if doing so would expedite the resolution of this case.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: _____

Bradley M. Knepper
Registration No. 44,189
1560 Broadway, Suite 1200
Denver, CO 80202-5141
(303) 863-9700

Date: March 3, 2005